

John R. Benson
HSEMD

Andy Buffington
Communications Center

Vacant
EMS

Larry Smith
Emergency Management

Vacant
Member At-Large

Ellen Hagen
Fire Department (Volunteer)

Rob Rotter
Sheriff's Office

Michael Kasper
Sheriff's Office

Vacant
Fire Department

Tom Lampe
Iowa DPS

Jason Leonard
Municipal Police Department

Carole Lund-Smith
ILEA

David Ness
Municipal Police Department

Denise Pavlik
Communications Center

Marty Smith
Iowa DPH

Sandra Black
Iowa DOT

Jeffery Sweargin
Iowa DNR

Patrick Updike
Iowa DOC

Bob von Wolffradt
Office of the CIO

Legislative Members
Senator Jim Lykam
Senator Randy Feenstra
Representative Bob Kressig
Representative Steven Holt

Dear P25 User Needs Subcommittee Chair,

The Iowa Statewide Interoperable Communications System Board (ISICSB) is tasked under Iowa Code 80.28 and 80.29 to ensure that interoperable capabilities among all public safety and public service entities in Iowa is as robust as technically and procedurally possible. With the completion of the new P25 Phase II Iowa Statewide Interoperable Communications System (ISICS) nearing, the Encryption Subcommittee (ESC) was commissioned to examine the need and technical requirements of deploying encrypted interoperable talkgroups on a statewide LMR system.

The ESC began meeting in August of 2017 and has steadily worked through various aspects of the deployment, management and operational implications of AES-256 encrypted interoperable talkgroups. The working sessions included meetings with technical experts from TR-8, the Federal Partnership for Interoperable Communications, and stakeholders at the local, state and federal level. The ESC discovered several technical obstacles that would hinder effective management of the various key material and update cycles.

Given those results, the ESC has drafted a white paper (enclosed) outlining the need for effectively managed encrypted interoperability in Iowa, technical and logistical limitations of the current communications landscape in Iowa and proposed solutions for the obstacles. The proposed solutions would enhance interoperability and benefit the entire P25 user base on a local, state and federal level.

This letter is submitted as an official request for consideration of the proposed solutions outlined below and in the included white paper. We encourage the UNS to consider these solutions to be forwarded to the Project 25 Steering Committee for consideration to be forwarded to the Telecommunications Industry Association (TIA) TR8 Chair for consideration and assignment to the appropriate subcommittees for possible action within the current suite of P25 standards relating to encryption.

1. Standardization and adoption of over-the-ethernet keying (OTEK) and over-the-Internet keying (OTIK) that would allow for the loading and updating of TEKs and KEKs, setting initial and modifying management periods, ability to interface with multiple key management devices and ability for a Master KMF to create and modify partitions on a crypto module;
2. Adoption of the Inter-KMF Interface to allow for agencies with disparate KMFs to securely share encryption material;
3. Standardization adoption of methods for subscriber radios to communicate with multiple KMFs. This includes the ability to define the home system KMF as the Master KMF and the others as secondary KMFs. This would also create a pathway for aliased SLNs to add flexibility in programming and partitioning of the crypto module.

John R. Benson
HSEMD

Andy Buffington
Communications Center

Vacant
EMS

Larry Smith
Emergency Management

Vacant
Member At-Large

Ellen Hagen
Fire Department (Volunteer)

Rob Rotter
Sheriff's Office

Michael Kasper
Sheriff's Office

Vacant
Fire Department

Tom Lampe
Iowa DPS

Jason Leonard
Municipal Police Department

Carole Lund-Smith
ILEA

David Ness
Municipal Police Department

Denise Pavlik
Communications Center

Marty Smith
Iowa DPH

Sandra Black
Iowa DOT

Jeffery Sweargin
Iowa DNR

Patrick Updike
Iowa DOC

Bob von Wolffradt
Office of the CIO

Legislative Members
Senator Jim Lykam
Senator Randy Feenstra
Representative Bob Kressig
Representative Steven Holt

These topics are introduced for discussion and we realize further work will be needed before a formal recommendation is considered for approval, but we believe these solutions would enhance the interoperable capabilities of numerous agencies whose personnel must utilize multiple P25 LMR systems.

If you have any questions, please direct them to our statewide interoperability coordinator, Chris Maiers, via email at maiers@dps.state.ia.us or via phone 515-201-7478.

Very respectfully,

Lieutenant Tom Lampe
Iowa Department of Public Safety
ISICSB Chair

Captain Jason Leonard
Waverly Police Department
ISICSB Vice Chair

Patrick Updike
Iowa Department of Corrections
ISICSB Technology Committee Chair